

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 04-268844
 (43)Date of publication of application : 24.09.1992

(51)Int.Cl. H04L 9/00
 H04L 9/10
 H04L 9/12
 G06F 15/00
 G09C 1/00

(21)Application number : 03-028602
 (22)Date of filing : 22.02.1991

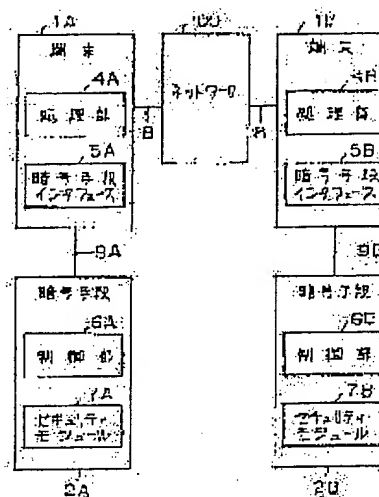
(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
 (72)Inventor : MIYAGUCHI SHOJI
 MORITA HIKARI

(54) CIPHER USING METHOD AND MEANS THEREFOR

(57)Abstract:

PURPOSE: To make a ciphering method to be used differ for every user.

CONSTITUTION: When at a terminal 1A, a ciphering means 2A is given the instruction of a key sharing method, the ciphering means 2A ciphers a common key KS2 by an initial key KS1, and sends this cipher text C2 to the terminal 1B. The terminal 1A sends C2 to the terminal 1B, and the terminal 1B sends C2 to the ciphering means 2B. The ciphering means 2B decodes C2 by the initial key KS1, and obtains the common key KS2. In the terminals 1A and 1B, data is cipher-processed by the common key KS2 by each ciphering means 2A, 2B, and is sent to the terminal, and is sent to an opposite party. The ciphering means 2A, 2B can be exchanged to the terminals 1A, 1B, and another ciphering method can be used by exchanging the ciphering means. The terminal can not know what ciphering program is used.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平4-268844

(43) 公開日 平成4年(1992)9月24日

(51) Int.Cl. ⁵	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 9/00				
9/10				
9/12				
G 0 6 F 15/00	3 3 0 F	7323-5L		
		7117-5K		
			H 0 4 L 9/00	Z
審査請求 未請求 請求項の数 2 (全 7 頁) 最終頁に続く				

(21) 出願番号 特願平3-28602

(22) 出願日 平成3年(1991)2月22日

(71) 出願人 000004226

日本電信電話株式会社
東京都千代田区内幸町一丁目1番6号

(72) 発明者 宮口 庄司

東京都千代田区内幸町一丁目1番6号 日
本電信電話株式会社内

(72) 発明者 森田 光

東京都千代田区内幸町一丁目1番6号 日
本電信電話株式会社内

(74) 代理人 弁理士 草野 卓

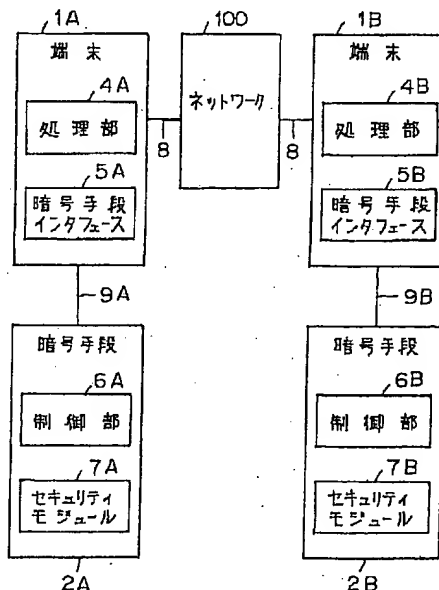
(54) 【発明の名称】 暗号利用方法とその暗号手段

(57) 【要約】

【目的】 利用者ごとに利用暗号方法を異ならすことを可能とする。

【構成】 端末1Aで暗号手段2Aに鍵共有方法を指示すると、暗号手段2Aは初期鍵KS1で、共通鍵KS2を暗号化し、その暗号文C₂を端末1Aへ送る。端末1AはC₂を端末1Bへ送り、端末1BはC₂を暗号手段2Bへ送る。暗号手段2BはC₂を初期鍵KS1で復号して共通鍵KS2を得る。端末1A、1Bではそれぞれその暗号手段2A、2Bでデータを共通鍵KS2で暗号処理し、端末へ送り、相手方へ送る。暗号手段2A、2Bは端末1A、1Bに対し交換可能であり、暗号手段を取替えて他の暗号方法を利用できる。端末はどのような暗号プログラムか知ることはできない。

図 1



1

【特許請求の範囲】

【請求項1】 端末利用者が、端末間で暗号を利用する暗号利用方式において、それぞれの端末に暗号手段を取外し自在に結合し、それぞれの暗号手段は制御部とセキュリティモジュールとからなり、そのセキュリティモジュールは、端末利用者が予め個別に適宜決めて搭載してある一個以上の暗号処理機能を含み、端末は、データを暗号手段に転送して暗号処理し、その暗号処理されたデータを返却してもらうことを特徴とする暗号利用方法。

【請求項2】 請求項1の暗号利用方法において、上記暗号手段は、マイクロプロセッサと、暗号LSI、暗号プログラムのいづれかの一個以上とを搭載するICカードや光カードからなることを特徴とする暗号手段。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 この発明は、ネットワークに加入した電話機、ファックス端末、テレックス端末、自動車電話機などの様々な端末が、秘密にするためにデータを暗号化して伝送するためや、データに対するデジタル署名をするためや、データが改ざんされているかの確認のために暗号を利用する方法に関する。

【0002】

【従来の技術】 従来の暗号利用方法を図3を参照して説明する。ネットワーク（通信網）100にはこれに加入した電話機101、ファックス端末102、テレックス端末103、自動車電話機104、個人携帯電話機105、パーソナルコンピュータ106、電子計算機107、データ通信端末108などの端末が接続されている。これら端末は、互いに暗号通信したり、或は、暗号を応用した信頼性の高い通信、つまりデジタル署名、データ改ざん有無の確認など暗号を利用した通信を行なう。ネットワーク100は、国内ネットワークや、国際ネットワークである。端末間で暗号通信を行うには、同じ暗号を使わなければならない。このためには、各端末が共通の暗号化および復号化手段をもつ必要がある。

【0003】 しかし次のような問題がある。即ち、①暗号はISO等で国際標準化が行われていない、このため、国際的な規模で、各端末が共通に使える暗号が存在しない、②端末によっては暗号化手順が秘密の暗号を利用したい、③暗号が破れた場合は、直ちに他の暗号に切り替えたい、等の暗号利用上の問題や要求がある。従来の暗号利用上の問題や要求に答えられる暗号方式、即ち、ネットワークに加入した全ての端末が共通の暗号を使わなくともよく、暗号化手順が秘密の暗号を利用でき、更に、暗号の切り替えが容易に出来、しかも安全性が高い暗号の利用方法は提案されていなかった。

【0004】 この発明の目的は、ネットワークに加入した全ての端末が、共通の暗号を使わなくともよく、暗号化手順が秘密の暗号も、また、暗号化手順を公開した暗号も利用でき、暗号の切り替えが容易に出来、しかも安

2

全性が高い暗号利用方法を提供することにある。この発明の説明に先立ち、暗号に関する用語を説明する。

（暗号化と復号化、暗号アルゴリズム）暗号化とは、平文 p を、暗号化アルゴリズム E により、鍵 k_1 で暗号化し、暗号文 c を得ることを言う。これを、数式で次のように表す。

$$c = E(k_1, p)$$

復号化とは、暗号文 c を、復号化アルゴリズム D により、鍵 k_2 で復号化し、平文 p を得ることを言う。これを、数式で次のように表す。

$$p = D(k_2, c)$$

ここで、暗号化アルゴリズム E と復号化アルゴリズム D は対になっており、両者を併せて、単に、暗号アルゴリズムという。

【0005】 $k_1 = k_2$ であるとき、暗号アルゴリズムは、秘密鍵暗号アルゴリズム、または単に秘密鍵暗号という、 $k_1 \neq k_2$ であるとき、暗号アルゴリズムは、公開鍵暗号アルゴリズム、または単に、公開鍵暗号と呼ばれる。秘密鍵暗号では、 k_1 および k_2 を秘密にする。公開鍵暗号では、 k_1 を公開する。但し、 k_2 は秘密とする。

（鍵の共有）端末 T_i と T_j とが、同じ暗号鍵を持つことを鍵の共有という。鍵の共有方法は様々なものがあり、次に4つの鍵共有の方法を説明する。これは、この発明の実施例において引用する。

【0006】 第1の鍵共有方法は、端末 T_i と T_j が、共有する鍵 KS_1 を、予め端末内部のメモリに保持しておくことである。これは、例えば端末 T_i や T_j の所有者が、通信手段を使わずに、手操作で鍵 KS_1 をその端末に設定することで達成される。共有する鍵が1個の場合もあれば、複数の場合もある。複数の場合は、鍵に番号や名前をつけておいて共有する鍵を区別する。鍵 KS_1 を初期鍵という。

【0007】 第2の鍵共有方法は、秘密鍵暗号を用いて、セッション鍵 KS_2 を端末 T_i から T_j へ配送する方法である。即ち、端末 T_i は、セッション鍵 KS_2 を、初期鍵 KS_1 で暗号化し、即ち、 $C_2 = E(KS_1, KS_2)$ として、暗号文 C_2 を得て、この C_2 を端末 T_j に送る。端末 T_j は、 C_2 を復号化して、即ち、 $KS_2 = D(KS_1, C_2)$ として KS_2 を得る。端末 T_i と T_j は、予め暗号化アルゴリズム E と復号化アルゴリズム D を決めておき、これら暗号アルゴリズムの実現手段を保持している。

【0008】 第2の鍵共有の詳細は、例えば国際標準ISO8732に規定される。セッション鍵とは、通信セッションの都度変更する鍵を意味する。第3の鍵共有方法は、公開鍵暗号を用いて、セッション鍵 KS_3 を端末 T_i から T_j へ配送する方法である。端末 T_i は、セッション鍵 KS_3 を暗号化し、即ち、 $C_3 = E(KS_1, KS_3)$ として、暗号文 C_3 を得て、この C_3 を

端末T_jに送る。端末T_jは、C3を復号化して、即ち、 $KS3=D(KS1r, C3)$ としてセッション鍵KS3を得る。ここで、Eは公開鍵暗号の暗号化アルゴリズム、Dは公開鍵暗号の復号化アルゴリズムである。KS1_rは公開鍵、KS1_rは秘密鍵である。ここで示した鍵共有の詳細は、例えば、次の文献に解説される。

[0009] W. Diffie and Hellmann 'New direction in cryptography', IEEE Transactions, Information Theory, IT-22, 6, PP644-654, November 1976. 第4の鍵共有方法は、端末T_iとT_jの間でパラメータの変換値を変換し、セッション鍵KS4を計算する方法である。両者は鍵生成手段を持つ。これら鍵生成手段の機能を関数Fで表すと、

$$KS4 = F(G(p1), p2)$$

である。ここで、p1とp2は、鍵生成手段に与えるパラメータであり、G(p1)やG(p2)は、パラメータの変換値である。関数FとGは、 $F(G(p1), p2) = F(G(p2), p1)$ となる性質を有する関数であり、更に、G(p1)からp1の値を求めること、及び、G(p2)からp2の値を求めることは、事実上不可能である。例えば、大型計算機を何千年間連続運転しても、p1やp2を求められないという性質を有する。

[0010] 端末T_iは、端末T_iのパラメータR_iを決め、パラメータの変換値G(R_i)の値を端末T_jへ送信し、端末T_jは、端末T_jのパラメータR_jを決め、パラメータの変換値G(R_j)の値を端末T_iへ送信する。端末T_iとT_jは、自己のパラメータと相手から送られてきたG(R_j)またはG(R_i)を用い、端末T_iは、 $KS4 = F(G(R_j), R_i)$ の計算により、端末T_jは、 $KS4 = F(G(R_i), R_j)$ の計算により、セッション鍵KS4を共有できる。パラメータを交換して鍵共有する方法は様々なものがあり、詳細は、例えば、文献、暗号と情報セキュリティの第4章(辻井重男編、昭晃堂、1990年)に、端末の名称(ID)を用いた鍵の共有方法として解説される。

(認証子の生成機能と認証子の確認機能) 通信上のデータが改ざんされているか否かを検出するため、32ビットの認証子を用いたデータ改ざんの検出機能は、データ改ざん検出関数G_{MAC}を用い、認証子の生成機能と認証子の確認機能により達成される。

[0011] データ改ざん検出関数G_{MAC}は、鍵KSと、長いデータDTとを入力し、32ビット長の認証子(MAC)を出力する。これを数式で書くと、

$$MAC = G_{MAC}(KS, DT)$$

認証子(MAC)は、鍵KSと、データDTとに依存して定まる性質を持つ特徴を持つ。関数G_{MAC}は、暗号化アルゴリズムを用いてつくられ、この暗号化アルゴリズムに入力する鍵が、データ改ざん検出関数G_{MAC}に入力

する鍵であり、この暗号化アルゴリズムに入力する平文が、データ改ざん検出関数G_{MAC}に入力するデータである。データ改ざん検出関数G_{MAC}の具体的な作り方は、例えば、国際標準ISO9797に規定される。

(データの改ざん検出) 端末T_iとT_jは、鍵KSと、データ改ざん検出関数G_{MAC}の実現手段を持つ。端末T_iが、データXを、端末T_jに送るとする。端末T_iは、鍵KSとデータXを関数G_{MAC}に入力し、認証子MAC1を生成する。即ち、 $MAC1 = G_{MAC}(KS, X)$ とする。次に、端末T_iは、データXとMAC1とを通信回線を経由して、端末T_jに送る。端末T_jは、データXとMAC1を受信し、自からも認証子を生成する。これをMAC2で表すと、 $MAC2 = G_{MAC}(KS, X)$ となる。端末T_jは、MAC1とMAC2とが一致すれば、即ち、 $MAC1 = MAC2$ として、データXが通信の途上で改ざんされなかったことが確認できる。データXがX'に変化していると、即ち、 $X \neq X'$ であるため、 $MAC1 \neq MAC2$ となり、データが通信途上で改ざんされたことが確認できる。

(データ圧縮機能) 長いデータ、例えば64×nビットや128×nビット長のデータを、64ビットや128ビットにデータ圧縮する機能であり、ハッシュ関数ともいう。データ圧縮機能は、例えば国際規格ISO10118に規定される。

[0012] その他特に説明しないが暗号を利用したデジタル署名もある。

[0013]

【課題を解決するための手段】この発明によれば各端末に暗号手段が取外し自在に取付けられ、各暗号手段は制御部とセキュリティモジュールとからなり、制御部の機能は標準化しておき、セキュリティモジュールは、端末利用者が個別に必要とする暗号処理機能、例えば手順非公開の秘密暗号のプログラムや暗号LSIチップや、手順公開暗号のプログラムや暗号LSIチップ等を、予め個別に適宜決めて搭載してある。端末はデータを暗号手段に転送して暗号処理をしてもらい、その暗号処理済みのデータを返却してもらう。

[0014] 端末利用者毎に暗号手段の暗号方法を個別化することにより、暗号手段を交換して端末間で、様々な暗号の切り替えが容易に出来、しかも暗号処理は暗号手段で行われ、端末自体はどのような暗号が利用されているか不明であり、安全性が高い。

[0015]

【実施例】図1にこの発明の実施例を示す。端末1A、1Bはネットワーク100に加入しており、この発明では端末1A、1Bにそれぞれ暗号手段2A、2Bが取外し自在に取付けられる。端末1Aは処理部4A、暗号手段インタフェース5Aを備え、暗号手段2Aは制御部6A及びセキュリティモジュール7Aを備えている。同様に、端末1Bは処理部4B、暗号手段インタフェース5

Bを備え、暗号手段2Bは制御部6B、セキュリティモジュール7Bを備えている。端末1A、1Bは通信回線8でネットワーク100に接続されている。端末1A、1Bはそれぞれ暗号手段2A、2Bと結合線9A、9Bで結合されている。ここで、結合線9Aは、端末1Aと暗号手段2A間でデータの流れがあること、また結合線9Bは、端末1Bと暗号手段2B間でデータの流れがあることを表す。暗号手段インタフェース5Aや5B、及び、制御部6Aや6Bの機能は、例えばCCITやISO等の国際的な範囲で標準化して用いる。

【0016】処理部4Aと4Bは、端末としての本来の機能を持つ。例えば、端末1Aや1Bが電話機であるとき、処理部4Aや4Bは電話機としての本来の機能を有し、端末1Aや1Bがファックス端末であるときは、ファックス端末としての本来の機能を有し、端末1Aや1Bがパソコンであるときは、パソコンとしての本来の機能を有す。端末1Aと端末1Bは、通信回線8とネットワーク100とを経由して通信する。暗号手段2Aや2Bは、マイクロプロセッサと、暗号LSIや暗号プログラムのメモリチップのいずれかの一個以上とを搭載するICカードや光カードなどの携帯が容易なものにより構成される。暗号手段インタフェース5Aや5Bは、ICカードあるいは光カードなどの暗号手段とのインタフェース処理部である。ここで光カードとは、光記憶部とマイクロプロセッサとを、1枚のカードに搭載したものを含む。制御部6Aや6Bは、それぞれ、セキュリティモジュール7Aや7Bが提供する機能を選択する機能と暗号手段インタフェース5Aや5Bとのインタフェースを受持つ。セキュリティモジュール7Aや7Bは、暗号処理機能、つまり暗号化、復号化機能、認証子の生成機能、認証子の確認機能、デジタル署名機能、署名検証機能のいずれかの機能を少なくとも一以上実現する手段と、更に必要に応じて鍵共有機能、データ圧縮機能などを含む。制御部6Aや6Bでは、例えば、選択番号1-1は、鍵共有方法1の機能を選択する、選択番号1-2は、鍵共有方法2の機能を選択する、・・・、選択番号2-1は、秘密鍵暗号Qの暗号化の機能を選択する、選択番号2-2は、FEAL暗号の暗号化機能を選択する、・・・、選択番号6はデータ圧縮機能を選択する、等と決めてあり、この決め方は例えば国内規格として標準化して使う。

【0017】図2に、暗号手段2Aのやや詳しい実施例を示す。セキュリティモジュール7Aは、暗号化の実現手段、復号化の実現手段、認証子の生成実現手段、認証子の確認の実現手段のいずれかを1個以上複数含み、更に場合によると鍵共有手段やデータ圧縮手段などを含む。鍵共有の実現手段は、例えば、鍵共有の方法1や、鍵共有の方法2や、鍵共有の方法3や、鍵共有の方法4を行うためのプログラムを含み、更に、鍵共有のための補助機能、例えば乱数の生成機能などを含む。セキュリ

ティモジュール7Aは、鍵共有方法1の初期鍵KS1を記憶している。初期鍵を複数保持する場合もあり、この場合は、複数の初期鍵を、番号あるいは名前により区別する。また、鍵共有方法2のセッション鍵KS2を記憶するメモリを含む。暗号化実現手段は、例えば、秘密暗号Qの暗号化プログラムやDES暗号の暗号化プログラムであり、あるいは、暗号化モードで動作するRSA暗号のチップである。復号化実現手段は、例えば、秘密暗号Qの復号化プログラムやDES暗号の復号化プログラムであり、あるいは、復号化モードで動作するRSA暗号のチップである。この場合、RSAチップは、ICカードあるいは光カードに搭載されており、秘密暗号やDES暗号のプログラムは、プロセッサに内蔵されたメモリに記憶されている。認証子の生成実現手段や認証子の確認の実現手段は、例えば、認証子生成プログラムや認証子の確認プログラムであり、プロセッサに内蔵されたメモリに記憶されている。ここで、秘密暗号Qとは、暗号手段2Aや2Bを使う者が独自に定めた暗号化手順を公開しない暗号を意味する。データ圧縮手段は、例えば、国際規格ISO10118等で規定するデータ圧縮機能のプログラムであって、例えば、プロセッサに内蔵されたメモリに記憶されている。以上述べたセキュリティモジュール7Aや7Bの暗号処理機能は、端末の利用者が予め個別に適宜決める。

【0018】次に、この発明の暗号利用方法により、端末1Aと端末1Bの間における、暗号通信や暗号を応用した通信方法を説明する。最初に端末1Aが、第2の鍵共有の方法で端末1Bとセッション鍵KS2を共有後、平文データXを秘匿して、端末1Bに送る例を説明する。端末1Aの処理部4Aは、暗号手段インタフェース部5Aを経て、制御部6Aに、第2の鍵共有方法により、端末1Bと鍵共有する機能を選択するように指示する。制御部6Aは、セキュリティモジュール7Aの内部にある第2の鍵共有方法を選択する。すると、セキュリティモジュール7Aは、端末1Bと予め共有している初期鍵KS1を、セキュリティモジュール7Aの記憶部から取り出し、次に乱数Rを生成する。セキュリティモジュール7Aは、乱数Rを、端末1Aと端末1B間の暗号通信用のための共有鍵KS2と定め（以降、セッション鍵KS2という）、即ち、 $KS2=R$ とし、このKS2を、セキュリティモジュール7Aの内部に記憶しておく。次に、このセッション鍵KS2を、初期鍵KS1で暗号化し、即ち、 $C2=E(KS1, KS2)$ として、セッション鍵KS2の暗号文C2を得て、このC2を制御部6Aを経て、更に、暗号手段インタフェース部5Aを経て、処理部4Aに送る。

【0019】処理部4Aは、暗号文C2を通信回線8を経て、端末1Bに送信する。端末1Bの処理部4Bは、暗号文C2を受信する。処理部4Bは、暗号手段インタフェース部5Bを経て、制御部6Bに、第2の鍵共有方法

7

により鍵共有する機能を選択することの指示と共に、受信した暗号文C2を伝える。制御部6Bは、セキュリティモジュール7Bに対して、第2の鍵共有方法により鍵共有の選択指示と暗号文C2を伝える。すると、セキュリティモジュール7Bは、まず端末1Aと共有している初期鍵KS1を、セキュリティモジュール7Bの記憶部から取り出し、次に暗号文C2を、鍵KS1で復号化し、即ち、 $KS2=D(KS1, C2)$ として、セッション鍵KS2を得る。セキュリティモジュール7Bは、共有したセッション鍵KS2をその内部に記憶しておく。セキュリティモジュール7Bは、制御部6Bを経て、セッション鍵KS2を共有したことを、処理部4Bに知らせる。処理部4Bは、セッション鍵KS2を共有したことを、通信回線8を経て、端末1Aの処理部4Aに知らせる。以上で、端末1Aと端末1B間で、セッション鍵KS2の共有を完了した。次に、端末1Aの処理部4Aが、平文データXを暗号文に変えて、端末1Bの処理部4Bに伝える暗号通信を説明する。

【0020】端末1Aの処理部4Aは、暗号手段インタフェース部5Aを経て、制御部6Aに、平文Xを暗号化する機能を選択するよう指示する。制御部6Aは、処理部4Aの指示に従い、平文Xをセキュリティモジュール7Aに伝える。すると、セキュリティモジュール7Aは、前記の方法で共有したセッション鍵KS2を、セキュリティモジュール7Aの記憶部から取り出し、平文Xをセッション鍵KS2で暗号化し、即ち、 $C3=E(KS2, X)$ として、暗号文C3を得て、このC3を制御部6Aを経て、更に、暗号手段インタフェース部5Aを経て、処理部4Aに送る。処理部4Aは、暗号文C3を、通信回線8を経て、端末1Bに送信する。端末1Bの処理部4Bは、暗号文C3を受信する。処理部4Bは、暗号手段インタフェース部5Bを経て、制御部6Bに、復号化の機能を選択する指示と共に、受信した暗号文C3を伝える。制御部6Bは、セキュリティモジュール7Bに対して、暗号文C3を復号化することを伝える。すると、セキュリティモジュール7Bは、前述した方法で共有したセッション鍵KS2を、セキュリティモジュール7Bの記憶部から取り出し、次に暗号文C3を、セッション鍵KS2で復号化し、即ち、 $X=D(KS2, C3)$ として、暗号文C3を復号化して平文Xを得る。セキュリティモジュール7Bは、制御部6Bを経て、復号化して得た平文Xを、処理部4Bに知らせる。

【0021】以上の説明は、鍵共有と暗号化および復号化が選択された例である。上記の説明において、セッション鍵KS2を共有後、処理部4Aが、認証子の生成機能を指示する場合は、セキュリティモジュール7Aの認証子生成手段が選択され、平文Xに対して、認証子MAC1を生成し、即ち、 $MAC1=G_{KAC}(KS2, X)$ とし、平文XとMAC1とが、端末1Aから、端末1B

8

に送られる。次に、端末1Bの認証子の確認手段が選択され、認証子MAC1が正しいか否かが調べられる。

【0022】この暗号利用方法を利用する者A(B)は、自己の暗号手段2A(2B)を携帯し、そのセキュリティモジュール7A(7B)の内部に、例えば、秘密暗号 Q_{A1} のプログラムと、RSA暗号のプログラムとを組み込む。更に、この暗号利用方法の利用者Aは、自己の他の暗号手段2A'を持ち、そのセキュリティモジュール7A'の内部に、自己が必要とする手段、例えば、秘密暗号 Q_{A1} のプログラムを組み込む。この暗号利用方法の他の利用者Bは、自己の暗号手段2B'を持ち、その内部に秘密暗号 Q_{B1} のプログラムを組み込む。ここで、秘密暗号 Q_{A1} は、利用者AとBの間で使う秘密暗号であり、秘密暗号 Q_{B1} は、利用者AとBの間で使う秘密暗号である。このようにすると、利用者Aと利用者Bは、秘密暗号 Q_{A1} とRSA暗号を内蔵する暗号手段を使って暗号通信が出来、また、利用者Aと利用者Bは、秘密暗号 Q_{B1} を内蔵する暗号手段を使って暗号通信が出来る。ここで、RSA暗号は、暗号化アルゴリズムと復号化アルゴリズムが公開された、即ち、暗号化手順が公開された暗号である。

【0023】以上述べたように、ネットワークに加入する端末の利用者は、それぞれ、自己が必要とする暗号の機能(例えば、鍵共有の機能、暗号化の機能、復号化の機能、認証子の生成機能、認証子の確認機能、データ圧縮機能で、その機能は利用者が規定出来る)を内蔵した、いわば利用者毎に個別化された暗号手段2A(2B)を持つ。また、暗号手段インタフェース部5Aや5Bは標準化してあるので、利用者毎に個別化された暗号手段2Aや2Bは、どの端末1Aや1Bとでも、結合して用いることが出来る。暗号の切り替えは、個別化された暗号手段を交換することにより達成できる。

【0024】

【発明の効果】以上の実施例から明らかなように、この発明によれば暗号の利用者は、自己の用途のために個別化された暗号手段を用いることにより、自己が必要とする暗号の利用が可能である。この理由から、ネットワークに加入した全ての端末が、共通の暗号を使わなくともよく、暗号化手順が秘密の暗号も、また、暗号化手順を公開した暗号も利用でき、暗号の切り替えが容易に出来る暗号の使い方が可能である。しかも暗号処理は各暗号手段で行われ、これを端末で知ることができないから、高い安全性が得られる。

【図面の簡単な説明】

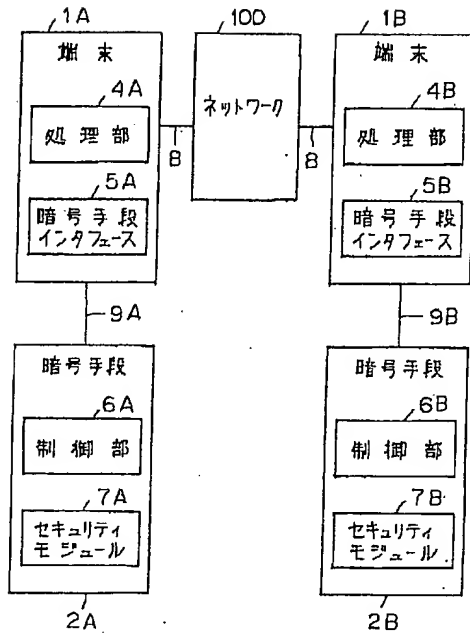
【図1】この発明の実施例を示すブロック図。

【図2】暗号手段2Aの具体例を示すブロック図。

【図3】ネットワークを介した端末間通信の一般的構成を示すブロック図。

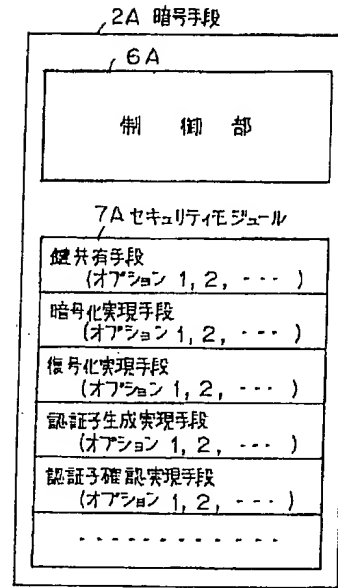
【図1】

図 1



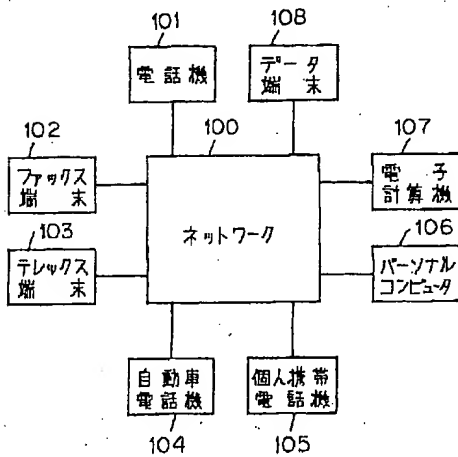
【図2】

図 2



【図3】

図 3



(7)

特開平4-268844

フロントページの続き

(51) Int. Cl.⁵

G09C 1/00

識別記号

庁内整理番号

7922-5L

F I

技術表示箇所

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☒ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.